IN THE CLAIMS:

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

1. – 66. (cancelled)

67. (currently amended) An apparatus, comprising:

a virus scanner adapted to scan a file stored in a storage device for infection with a virus;

a quarantining device adapted to quarantine the file from non-infected files on the storage device, when the file is infected; and

a converting device adapted to convert the quarantined file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

68.- 74. (cancelled)

75. (currently amended) An apparatus comprising:

a storage device adapted to store a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device adapted to input a selected file with infected status;

a quarantining device adapted to quarantine the selected file on the storage device; and

a converting device adapted to convert the selected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

76. - 78. (cancelled)

79. (currently amended) An apparatus, comprising:

a storage device adapted to store a plurality of files and a status for each of the files indicating whether each of the files is infected with a virus;

an input device adapted to input a selected file to be converted; and

a converting device adapted to convert the selected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

80.-83. (cancelled)

84. (currently amended) A method, comprising:

scanning a file for infection with a virus using a computer;

quarantining the file from non-infected files if the file is infected with a virus; and

converting the file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

85.- 93. (cancelled)

94. (previously presented) A computer readable storage medium controlling a computer by:

scanning a file for infection with a virus;

quarantining the file if infected with a virus; and

converting the quarantined file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

95.- 108. (cancelled)

109. (previously presented) A method comprising:

scanning a file for infection with a virus using a computer;

isolating the file from non-infected files, if the file is infected with a virus; and

converting the infected file into encoded data by executing an encoding process that converts an infected file in an infected condition into another encoded data when the infected file is detected.

110. - 144. (cancelled)

145. (new) A method for performing an anti-virus operation, the method comprising:
detecting a virus-infected file in a storage device using a computer;
converting the virus-infected file into encoded data; and
storing the encoded data of the virus infected file.

146. (new) The method according to claim 145 further comprising:
executing inverse conversion of said encoded data for restoring the virus-infected file.

147. (new) The method according to claim 145 further comprising:
registering virus information of the virus-infected file in an infection management table.

148. (new) The method according to claim 147 further comprising:
outputting the virus information for a virus analysis.

149. (new) The method according to claim 145 wherein an operation of said detecting is activated periodically or activated in response to a command instruction.

150. (new) The method according to claim 145 wherein the encoded data is stored in a different storage area from a storage area in which the virus-infected file was stored.

151. (new) The method according to claim 145 wherein the encoded data is stored in a storage area which cannot be accessed readily.

152. (new) The method according to claim 147, further comprising:
deleting the virus information of the virus-infected file registered in the infection management table through an interactive process.

153. (new) The method according to claim 147 wherein the virus information contains a virus name and a storage location in which the virus-infected file was stored.